World Agroforestry Centre Policy Series MG/C/4/2012

Use of Mobile Devices on Voice and Data Networks Policy

One of the policies on information security and business continuity which will be audited by the CGIAR Internal Audit Unit for all Centres given (a) their network inter-linkage through Active Directory and (b) the inter-reliance of many Centres for information backup and recovery of hosted outreach sites.

Document Revision History

Version	Date	Author(s)	Revision Notes
1.0	20/05/2012	Ian Moore	First draft circulated to staff
1.1	30/8/2012	Ian Moore, Rosemary Kande	Final version Approved by SLT

Document Control

The Head, ICT of the common services unit providing ICT Services to the World Agroforestry Centre (ICRAF) and the International Livestock Research Institute (ILRI) will maintain control of the document which will be reviewed every two years in conjunction with the ICT Steering Group.

Proposed updates will be presented to the Centres' senior management for adoption according to their organizational arrangements for approval of ICT policies. Upon acceptance by the Centres, the update will come into force.

Any discretionary controls added by a Centre may be reviewed annually; however updates may occur more frequently if deemed necessary.

Purpose

The purpose of this document is to communicate the Centre's policy on using mobile devices and external voice (mobile networks) and data (internet) networks. It should be read in conjunction with the document "Guidelines on the assignment, cost allocations, security and acceptable use of mobile devices on voice and data lines and external internet connections". The policy is in place to define eligibility on who is entitled to use official mobile services, to clearly indicate the assignment of costs incurred and to outline acceptable use to protect the employee and the Centre. Inappropriate use can expose the Centre to risks at both a technical level (with potential damage being caused to ICT infrastructure) and at operational level (excessive cost or misuse of mobile devices on the internet leading to possible reputational damage to Centres and loss in productivity).

The Centre's intentions for publishing a Use of Mobile Devices on External Voice and Data Networks Policy are not to impose restrictions that are contrary to the Centre's established culture of openness, trust and integrity. The Centre is committed to protecting its employees, partners and the organization from illegal or damaging actions by individuals, either knowingly or unknowingly.

Effective security is a team effort involving the participation and support of every Centre employee and affiliate who deals with information and/or information systems. It is the responsibility of every user of World Agroforestry mobile voice and data services to know these guidelines, and to conduct their activities accordingly.

This policy will be reviewed by the CGIAR Internal Audit Unit (IAU). A shared CGIAR electronic network exists (through the implementation of Active Directory) and which as a result, created an inter-dependency among the Centres with regard to network security. It is therefore important that all Centres are reviewed against a common set of ICT security guidelines.

Scope

This document covers the eligibility, use and security of employees who use mobile phone services and internet connections (excluding the office or campus internet connections provided by the Centre) for work purposes; using both official or personal mobile devices[1] and services. The three principal areas covered are:

- Use of mobile devices that contain a SIM card to connect to mobile voice and data networks;
- Use of fixed internet services provided for home internet connectivity;

[1] See mobile device definition on page 5

- Connecting to the internet when on the move: using a mobile device to connect to the internet using wireless or Ethernet cable; using the official CGIAR Travellers Access Service (TAS) to connect to pay for use services; or using computers provided in internet cafés, business centres or partner organizations.

1. Eligibility

1.1. An official mobile voice and data line, home internet connection, or the CGIAR Travellers Access Service (TAS) can be provided to an employee where operational efficiency, quality of service, safety, or either of these are significantly improved.

1.2. In order for an official mobile voice, data line or home internet connection to be provided, the employee should provide justification and seek approval from the supervisor. Where the supervisor is not the budget holder, the supervisor will recommend and seek approval from the budget holder. All approved requests will be submitted to ICT Services (for services in Kenya) and country or regional administrators (country or regional offices) for processing. A valid budget code where official costs resulting from the one-time installation/setup fees and the monthly usage costs of the mobile voice and data line or internet connection will be charged should be provided by the budget holder.

1.3. The service will be obtained through the Centre's corporate account/plan from the mobile network or internet provider. In locations or situations where it is not feasible to use a corporate account/plan the employee will use a personal account and make an expense claim for entitled reimbursement.

1.4. By default voice and data roaming services will **NOT** be activated on lines in the corporate account. However, with adequate justification the budget manager can authorise ICT Services (for services in Kenya) or the relevant country/regional administrator (country or regional offices) to enable this service.

1.5. ICT Services will provide guidance on a recommended mobile device to use for the functions required. Mobile devices should be obtained as part of a monthly plan or through a loyalty agreement with the mobile service provider wherever possible. In cases where a mobile device is not provided or if a mobile device with different specifications is required, authorization to purchase the device will be given by the budget holder upon receipt of the approved justification either from the staff (where the budget holder is the supervisor), or the supervisor where s/he is not the budget holder.

1.6. Mobile devices owned by the employee may be used as long as all requirements on acceptable use and security mentioned in this and other Centre policies are met.

2. Clearance on employee exit

2.1. The official post-paid mobile line or home internet service will be terminated when the staff leaves the employment of the World Agroforestry Centre (on expiry of an employee's contract, following

resignation or for other reasons including death). An approval to retain the mobile line but on a personal post-paid or prepaid plan may be approved by the responsible director when requested by the employee. The ICT unit will then facilitate the migration to a personal prepaid or post-paid facility as per the exiting employee's preference.

2.2. An employee may keep a Centre-allocated mobile device that has been in use for two years or more. Where the device has been in use for less than two years, s/he may purchase it upon approval by the budget holder and on paying the Centre the value of the phone as assessed by the ICT unit. The value of the mobile device will be determined by its age and utility.

3. Costs

3.1. For all official use of voice and data networks or connections to the internet including Travellers Access Services (TAS) usage, the budget holder must provide a cost centre where the costs will be charged.

3.2. One-time installation or setup/configuration costs for approved mobile voice and data lines or internet at home will be charged to the cost centre provided. Payment will not be made retrospectively for equipment that is already owned by the employee. Where the Centre supports a Bring Your Own Device (BYOD) programme, the employee may receive financial assistance to purchase a personal mobile device in line with the programme's guidelines.

3.3. A maximum unaccountable amount for both mobile line usage and home internet connection monthly costs will be set for each location where World Agroforestry staff are based (duty station). The Senior Leadership Team (SLT) will approve a maximum unaccountable amount for employees based in Kenya. The ICT unit in liaison with the respective regional or country coordinators will make an analysis and recommend an appropriate unaccountable amount for each duty station. The Deputy Director General, Finance and Corporate Services and the Deputy Director General, Partnerships and Impact, will approve the recommended unaccountable amounts for each duty station. A budget manager may request in writing for a lower unaccountable amount to be implemented for mobile voice and data lines or for home internet connections for budgets that they manage.

3.4. Costs in excess of the maximum unaccountable amount are charged to the employee. Costs incurred through justifiable official use can be claimed as an expense with the approval of the direct supervisor and budget holder. The Centre reserves the right to recover amounts in excess of the maximum unaccountable amount from the employee's monthly salary.

3.5. To minimize the risk of excessively high monthly usage costs the Centre will set a maximum monthly limit. Wherever possible the service provider will be asked to immediately block further use of the mobile line or internet connection when the limit is reached. If this is not possible the service provider will alert the employee and ICT services when usage is excessively high or inform the employee how to check the current usage amount.

4. Acceptable use, applications and security

4.1. It is the responsibility of the employee to safeguard the mobile device and the SIM card of official mobile lines.

4.2. In case of loss of the mobile device or SIM card, through any means, the employee is required to immediately report the loss to ICT Services for prompt barring of the mobile line and to change passwords for services that can be used from the mobile device. The employee will be responsible for **ALL** costs incurred before the loss is reported, if the loss of the device and/or SIM card is **NOT** reported immediately.

4.3. It is the responsibility of the employee to safeguard the Centre's data stored on a mobile device. ICT Services will provide guidance to ensure all Centre data or information stored on a mobile device is backed up to a secure location.

4.4. ICT Services will support a standard set of applications that can be installed or configured on the mobile device. A secure connection should be used by applications that access Centre business systems. A list of applications that are known to contain malware or cause problems for the standard set of applications will be made available and should **NOT** be installed on the mobile device.

4.5. Employees should follow the guidelines provided to manage the significantly higher costs for voice and especially data services when roaming.

4.6. When using publicly provided computers or mobile devices (internet café or business centre) or those provided by partners; employees should access Centre business systems over a secure connection and ensure that all information saved to the computing device is deleted when the session is complete and that user names and passwords are never saved on the computer.

4.7. When using the internet from services that are fully or partially paid for by the Centre and where the service is provided through a corporate account employees are reminded to follow the guidelines laid out in the ICT Privacy and Acceptable Use Policy.

5. Related documentation

5.1. ICT Privacy and Acceptable Use Policy

5.2. Guidelines on the Assignment, Cost Allocation, Security and Acceptable Use of Mobile Devices on Voice and Data Lines and External Internet Connections

5.3. Network Infrastructure Security Policy

5.4. Network User Identification and Authentication Policy

5.5. Workstation Security Policy

5.6. Internet and Email Security Policy

6. Compliance and waivers

6.1. Compliance with this policy by users, network administrators, or others responsible for implementation of the policy, is mandatory. Procedures are in place to monitor compliance with this policy.

6.2. Violations of this policy may result in disciplinary action in accordance with the human resources policies of the Centre.

6.3. Requests for waivers of this policy shall be formally submitted to the director responsible in writing. The requests shall set out the justification, duration of the proposed waiver and how the increased risk arising from the waiver will be managed. Requests will be approved by the Director General upon recommendation by the director responsible, in consultation with the Head, ICT and will be documented.

6.4. Approved waivers shall be monitored to ensure that the conditions of the waivers are being observed.

Definitions

- **A mobile device:** can be a simple mobile phone for voice and basic data communications, a smartphone (Blackberry, iPhone, Android, Windows mobile etc.), a tablet or iPad, a netbook, notebook or laptop computer, a 3G (or other) modem or any other device that contains a SIM card.
- **Budget holder:** The person responsible for the management of a cost centre's budget.
- **Responsible director:** A member of the Senior Leadership Team who has responsibility for the person making the request.
- **TAS (Travellers Access Service)**: A CGNET service provided through iPass and installed on a Centre-owned laptop or mobile device and that enables employees to connect to paid wireless and dial-up internet connections in locations such as airports, hotels and coffee shops, without providing credit card details or making upfront payments.